



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/878,336	06/12/2001	Fujio Seki	122.1456	2145

21171 7590 06/29/2005  
STAAS & HALSEY LLP  
SUITE 700  
1201 NEW YORK AVENUE, N.W.  
WASHINGTON, DC 20005

EXAMINER

PICH, PONNOREAY

ART UNIT PAPER NUMBER

2135

DATE MAILED: 06/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/878,336

Applicant(s)

SEKI ET AL.

Examiner

Ponnoreay Pich

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 21 April 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-37 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

Claims 1-14, 16-18, 20-22, 24-26, 28-30, 32-34, and 36 were amended. Claim 37 was added. Claims 1-37 have been examined and are pending.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

### ***Response to Amendment***

The examiner notes the amendments to the abstract, specification, and claims. The examiner withdraws the previous office action's objection to the abstract in light of the amendments. The examiner withdraws the previous 112, second paragraph rejection of the claims in light of the amendments. The examiner does not withdraw the previous objections to the specifications. The examiner notes that the applicant made several changes to the specification which now makes previously incomprehensible portions of the specification comprehensible. However, several minor errors still exist in the specification which applicant did not fix, which the examiner assumes stemmed from a poor translation of the original text. While these errors do not render the specification completely incomprehensible like the errors that were fixed by the applicant, they do make the specification harder to read than necessary. See page 2 for instance: "In **the** light of the above problem...a user uses the private computer for **the** work that does not require the Internet or for **the** work that is particularly important...."

### ***Response to Arguments***

Art Unit: 2135

Applicant's arguments with respect to claim 1-35 have been considered but are moot in view of the new ground(s) of rejection. The examiner notes that these arguments stem from the amendments to the claims. See new rejections below.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 7, 13, 14-16, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beasley et al (US 5,721,842) in view of Crandall (US 5,159,632).

**Claim 1:**

Beasley discloses a switching device for controlling a connection between at least one private computer, at least one terminal corresponding to the at least one private computer, and a shared computer that can be operated by the at least one terminal (Fig 1), the switching device comprising:

1. A connecting unit that connects each terminal to a corresponding private computer in default status and switches a connection destination of the terminal to a private computer corresponding to said terminal or the shared computer when a connection switching request transmitted from said terminal has been received (col 2, lines 56-64).

Art Unit: 2135

2. A security unit that executes for each terminal identification processing of data that has been received from any one terminal and output to the private computer or the shared computer (col 1, lines 45-61 and col 3, lines 4-16).

Beasley does not disclose said identification processing including utilizing an identifier corresponding to a connector through which a terminal is connected to encipher a received key code. However, this limitation reads on the use of public key cryptography, which was well known at the time the applicant's invention was made. Public key cryptography is further disclosed by Crandall (col 1, lines 32-51). In public key cryptography, the key itself is an identifier and corresponds to or verifies the identity of the sender or connector from which a message is sent. The reason for this is that the public key is an inverse of the private key, so a message enciphered with one can only be deciphered with the other. If the deciphering is successful, it verifies the identity or source of the message (i.e. enciphered key code).

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Beasley's invention according to the limitations recited in claim 1. One of ordinary skill would have been motivated to incorporate Crandall's teachings as Crandall discloses that the use of public key encryption would eliminate the difficulties of exchanging a secure enciphering key (col 1, lines 32-34).

**Claim 7:**

Beasley discloses a switching method in a switching device for controlling a connection between at least one private computer, at least one terminal corresponding to the at least one private computer, and a shared computer that can be operated by the at least one terminal (Fig 1), the switching method comprising:

1. Connecting each terminal to a corresponding private computer in a default status and a connection destination of the terminal is switched to a private computer corresponding to said terminal or the shared computer when a connection switching request transmitted from said terminal has been received (col 2, lines 56-64).
2. Identification processing for each terminal executed on data that has been received from any one terminal and output to the at least one private computer or the shared computer (col 1, lines 45-61 and col 3, lines 4-16).

Beasley does not disclose said identification processing including utilizing an identifier corresponding to a connector through which a terminal is connected to encipher a received key code. However, this limitation reads on the use of public key cryptography, which was well known at the time the applicant's invention was made. Public key cryptography is further disclosed by Crandall (col 1, lines 32-51). In public key cryptography, the key itself is an identifier and corresponds to or verifies the identity of the sender or connector from which a message is sent. The reason for this is that the public key is an inverse of the private key, so a message enciphered with one can only

Art Unit: 2135

be deciphered with the other. If the deciphering is successful, it verifies the identity or source of the message (i.e. enciphered key code).

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Beasley's invention according to the limitations recited in claim 7. One of ordinary skill would have been motivated to incorporate Crandall's teachings as Crandall discloses that the use of public key encryption would eliminate the difficulties of exchanging a secure enciphering key (col 1, lines 32-34).

**Claim 13:**

Beasley discloses a computer system comprising at least one private computer; a terminal corresponding to the at least one private computer; at least one shared computer connected to a network; and a switching device disposed between the at least one private computer and the terminal, for relating data between the terminal and the shared computer (Fig 1), comprising:

1. A connecting unit that connects each terminal to a corresponding private computer in a default status and switches a connection destination of the terminal to a private computer corresponding to said terminal or the at least one shared computer when a connection switching request transmitted from said terminal has been received (col 2, lines 56-64).
2. A security unit that executes for each terminal identification processing on data that has been received from any one terminal and output to the at least one

Art Unit: 2135

private computer or the at least one shared computer (col 1, lines 45-61 and col 3, lines 4-16).

Beasley does not disclose said identification processing including utilizing an identifier corresponding to a connector through which a terminal is connected to encipher a received key code. However, this limitation reads on the use of public key cryptography, which was well known at the time the applicant's invention was made. Public key cryptography is further disclosed by Crandall (col 1, lines 32-51). In public key cryptography, the key itself is an identifier and corresponds to or verifies the identity of the sender or connector from which a message is sent. The reason for this is that the public key is an inverse of the private key, so a message enciphered with one can only be deciphered with the other. If the deciphering is successful, it verifies the identity or source of the message (i.e. enciphered key code).

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Beasley's invention according to the limitations recited in claim 13. One of ordinary skill would have been motivated to incorporate Crandall's teachings as Crandall discloses that the use of public key encryption would eliminate the difficulties of exchanging a secure enciphering key (col 1, lines 32-34).

**Claim 14:**

Beasley and Crandall do not explicitly disclose wherein at least one shared computer is connected to a second network independent of said network. However, the

Art Unit: 2135

examiner would like to take official notice that computer systems and networks wherein at least one computer (shared or private) that is connected to a further/second network independent of said network have existed before the time of the applicant's invention.

One of ordinary skill in the art would be motivated to connect a shared computer to a further independent network as this would allow more access of information for the users of the combination system of Beasley and Crandall. The examiner notes that the above notice was taken in the last office action and as applicant did not disagree with the statement, the examiner assumes that the applicant agrees with it.

**Claim 15:**

Beasley and Crandall do not explicitly disclose wherein the network is the Internet. However, the examiner would like to take official notice that a network being the Internet, which is connected to a computer of any sort has been known to exist before the time of the applicant's invention. One of ordinary skill in the art would be motivated to connect a shared computer to a further independent network as this would allow more access of information for the users of the combination system of Beasley and Crandall. The examiner notes that the above notice was taken in the last office action and as applicant did not disagree with the statement, the examiner assumes that the applicant agrees with it.

**Claim 16:**

Beasley and Crandall do not explicitly disclose wherein the second network is an intranet. However, the examiner would like to take official notice that a further/second network being an intranet has existed before the time of the applicant's invention. One

Art Unit: 2135

of ordinary skill in the art would be motivated to connect a shared computer to a further independent network as this would allow more access of information for the users of the combination system of Beasley and Crandall. Some of the information may be obtained only by being connected to the intranet. The examiner notes that the above notice was taken in the last office action and as applicant did not disagree with the statement, the examiner assumes that the applicant agrees with it.

**Claim 37:**

Beasley discloses a switching device for controlling a terminal connection (Fig 1), comprising:

1. A connection unit adapted to connect a terminal to a private computer or a shared computer (col 2, lines 56-64).

Beasley does not disclose an identification processing unit coupled to said connection unit and adapted to utilize an identifier corresponding to a connector through which said terminal is connected to encipher a received code. However, this limitation reads on the use of public key cryptography, which was well known at the time the applicant's invention was made. Public key cryptography is further disclosed by Crandall (col 1, lines 32-51). In public key cryptography, the key itself is an identifier and corresponds to or verifies the identity of the sender or connector from which a message is sent. The reason for this is that the public key is an inverse of the private key, so a message enciphered with one can only be deciphered with the other. If the

Art Unit: 2135

deciphering is successful, it verifies the identity or source of the message (i.e. enciphered key code).

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Beasley's invention according to the limitations recited in claim 37. One of ordinary skill would have been motivated to incorporate Crandall's teachings as Crandall discloses that the use of public key encryption would eliminate the difficulties of exchanging a secure enciphering key (col 1, lines 32-34).

Claims 2, 8, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beasley et al (US 5,721,842) in view of Crandall (US 5,159,632) and further in view of Ostermann et al (US 4,484,025).

**Claims 2 and 8:**

Beasley further discloses a unit and method wherein:

1. An encoding unit executes an encoding processing of each terminal executed on the data that has been transmitted from any one terminal and received by the switching device (col 1, last paragraph; col 2, lines 1-4; and col 3, lines 36-55).
2. A first decoding unit executes a decoding processing corresponding to the encoding processing of the terminal corresponding to the at least one private computer executed of the data that has been output from the switching device to any one private computer (col 1, lines 56-61 and Fig 1, item 70).

3. A second decoding unit that executes a decoding processing corresponding to the encoding processing of the terminal currently connected to the shared computer executed for data that has been output from the switching device to the shared computer (col 1, lines 56-61 and Fig 1, item 70). Note there are multiple decoding units disclosed by Beasley (Fig 1, items 70).

Beasley do not explicitly disclose that the encoded data are enciphered or deciphered. However, Ostermann discloses a system and method for transmitting data between two terminals or computers wherein the data are enciphered at the transmitting end and deciphered at the receiving end (abstract). Secure data transmission between two devices (as disclosed by Ostermann) was and still is a concern for one of ordinary skill in the art. One of ordinary skill would not only encode the transmitted data, but also encipher it for security purposes. Once the data arrives at the destination, only the intended recipient or system should be able to decipher the transmitted data. Therefore, one of ordinary skill would have been motivated to modify Beasley's invention according to the limitations recited in claims 2 and 8 for security purposes.

**Claim 17:**

Beasley discloses a computer system comprising at least one private computer; a terminal corresponding to the at least one private computer; at least one shared computer connected to a network; and a switching device disposed between the at least one private computer and the terminal, for relaying data between the terminal and the at least one shared computer (Fig 1), the switching device comprising:

1. A connecting unit that connects each terminal to a corresponding private computer in a default status and switches a connection destination of the terminal to a private computer corresponding to said terminal or the shared computer when a connection switching request transmitted from said terminal has been received (col 2, lines 56-64).
2. A security unit that executes for each terminal identification processing on data that has been received from any one terminal and output to the at least one private computer or the shared computer (col 1, lines 45-61 and col 3, lines 4-16).
3. An encoding unit executes an encoding processing of each terminal executed on the data that has been transmitted from any one terminal and received by the switching device (col 1, last paragraph; col 2, lines 1-4; and col 3, lines 36-55).
4. A first decoding unit executes a decoding processing corresponding to the encoding processing of the terminal corresponding to the at least one private computer executed of the data that has been output from the switching device to any one private computer (col 1, lines 56-61 and Fig 1, item 70).
5. A second decoding unit that executes a decoding processing corresponding to the encoding processing of the terminal currently connected to the shared computer executed for data that has been output from the switching device to the shared computer (col 1, lines 56-61 and Fig 1, item 70). Note there are multiple decoding units disclosed by Beasley (Fig 1, items 70).

Beasley do not explicitly disclose that the encoded data are enciphered or deciphered. However, Ostermann discloses a system and method for transmitting data between two terminals or computers wherein the data are enciphered at the transmitting end and deciphered at the receiving end (abstract). Secure data transmission between two devices (as disclosed by Ostermann) was and still is a concern for one of ordinary skill in the art. One of ordinary skill would not only encode the transmitted data, but also encipher it for security purposes. Once the data arrives at the destination, only the intended recipient or system should be able to decipher the transmitted data.

Beasley does not discloses said identification processing including utilizing an identifier corresponding to a connector through which a terminal is connected to encipher a received key code. However, this limitation reads on the use of public key cryptography, which was well known at the time the applicant's invention was made. Public key cryptography is further disclosed by Crandall (col 1, lines 32-51). In public key cryptography, the key itself is an identifier and corresponds to or verifies the identity of the sender or connector from which a message is sent. The reason for this is that the public key is an inverse of the private key, so a message enciphered with one can only be deciphered with the other. If the deciphering is successful, it verifies the identity or source of the message (i.e. enciphered key code). One of ordinary skill would have been motivated to incorporate Crandall's teachings as Crandall discloses that the use of public key encryption would eliminate the difficulties of exchanging a secure enciphering key (col 1, lines 32-34).

Art Unit: 2135

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Beasley's invention according to the limitations recited in claim 17. One of ordinary skill would have been motivated to do so for the reasons given above.

**Claims 18-20:**

Claims 18-20 recites limitations substantially similar to the ones recited in claims 14-16 respectively. As such, they are rejected for the same reasons.

Claims 3, 9, and 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beasley et al (US 5,721,842) in view of Crandall (US 5,159,632) and Ostermann et al (US 4,484,025) and further in view of Nelson, Jr. (US 5,675,653).

**Claims 3 and 9:**

Beasley, Crandall, and Ostermann do not explicitly disclose:

1. During the enciphering processing, the received data is bit shifted (by an enciphering unit) to a first direction between a highest bit and a lowest bit by only a number of each terminal.
2. During the first deciphering processing, the output data is bit shifted (by a first deciphering unit) to a second direction opposite to the first direction by a number of a terminal corresponding to the at least one private computer.

3. During the second deciphering processing, output data is bit shifted (by a second deciphering unit) to a second direction opposite to the first direction by a number of a terminal currently connected to the shared computer.

However, an enciphering unit in which data is encrypted by shifting bits in a first direction is not only known by one of ordinary skill in the art at the time of the applicant's invention, it is also disclosed by Nelson, Jr. (col 2, 1<sup>st</sup> paragraph). One of ordinary skill would recognize that to decrypt the encrypted data, one would need only to shift the bits of the encrypted data in a direction opposite the direction used to encrypt the data.

The examiner has interpreted "a number of a terminal" to include an encryption key uniquely associated with each terminal. The use of encryption key is well known by one of ordinary skill at the time of the applicant's invention and disclosed by Nelson, Jr. (col 5, lines 15-20). One of ordinary skill in the art would recognize that it would be more secure if the number of shifts done on each bit of data were determined in some manner by a terminal key or number. As the examiner interprets the claim, one possible purpose of enciphering data is so that if a computer accidentally receives data from a terminal when it was not supposed to, the computer would not be able to decode the data since it would not apply the correct number of bit shifts since the computer expected the data to come from one terminal and instead it came from another. In this manner, terminal data is secured as only when a terminal sends data to the correct computer and the computer uses the correct encryption key or number to decrypt the

Art Unit: 2135

data from the terminal it expected the data to come from would the computer be able to correctly interpret the data.

Claim 9 differs from claim 3 in that claim 3 discloses a switching unit which utilizes the steps disclosed by the method of claim 9.

**Claim 21:**

Beasley discloses a computer system comprising at least one private computer; a terminal corresponding to the at least one private computer; at least one shared computer connected to a network; and a switching device disposed between the at least one private computer and the terminal, for relaying data between the terminal and the at least one shared computer (Fig 1), the switching device comprising:

1. A connecting unit that connects each terminal to a corresponding private computer in a default status and switches a connection destination of the terminal to a private computer corresponding to said terminal or the shared computer when a connection switching request transmitted from said terminal has been received (col 2, lines 56-64).
2. A security unit that executes for each terminal identification processing on data that has been received from any one terminal and output to the at least one private computer or the shared computer (col 1, lines 45-61 and col 3, lines 4-16).
3. An encoding unit executes an encoding processing of each terminal executed on the data that has been transmitted from any one terminal and received by the switching device (col 1, last paragraph; col 2, lines 1-4; and col 3, lines 36-55).

4. A first decoding unit executes a decoding processing corresponding to the encoding processing of the terminal corresponding to the at least one private computer executed of the data that has been output from the switching device to any one private computer (col 1, lines 56-61 and Fig 1, item 70).
5. A second decoding unit that executes a decoding processing corresponding to the encoding processing of the terminal currently connected to the shared computer executed for data that has been output from the switching device to the shared computer (col 1, lines 56-61 and Fig 1, item 70). Note there are multiple decoding units disclosed by Beasley (Fig 1, items 70).

Beasley does not explicitly disclose that the encoded data are enciphered or deciphered. However, Ostermann discloses a system and method for transmitting data between two terminals or computers wherein the data are enciphered at the transmitting end and deciphered at the receiving end (abstract). Secure data transmission between two devices (as disclosed by Ostermann) was and still is a concern for one of ordinary skill in the art. One of ordinary skill would not only encode the transmitted data, but also encipher it for security purposes. Once the data arrives at the destination, only the intended recipient or system should be able to decipher the transmitted data.

Beasley does not disclose said identification processing including utilizing an identifier corresponding to a connector through which a terminal is connected to encipher a received key code. However, this limitation reads on the use of public key cryptography, which was well known at the time the applicant's invention was made.

Art Unit: 2135

Public key cryptography is further disclosed by Crandall (col 1, lines 32-51). In public key cryptography, the key itself is an identifier and corresponds to or verifies the identity of the sender or connector from which a message is sent. The reason for this is that the public key is an inverse of the private key, so a message enciphered with one can only be deciphered with the other. If the deciphering is successful, it verifies the identity or source of the message (i.e. enciphered key code). One of ordinary skill would have been motivated to incorporate Crandall's teachings as Crandall discloses that the use of public key encryption would eliminate the difficulties of exchanging a secure enciphering key (col 1, lines 32-34).

Beasley also does not disclose:

1. The enciphering unit for bit shifting the received data in a first direction between a highest bit and a lowest bit by a number of each terminal.
2. The first deciphering unit for bit shifting the output data to a second direction opposite to the first direction by a number of a terminal corresponding to the at least one private computer.
3. The second deciphering unit for bit shifting the output data to a second direction opposite to the first direction by a number of a terminal currently connected to the shared computer.

However, an enciphering unit in which data is encrypted by shifting bits in a first direction is not only known by one of ordinary skill in the art at the time of the applicant's invention, it is also disclosed by Nelson, Jr. (col 2, 1<sup>st</sup> paragraph). One of ordinary skill

Art Unit: 2135

would recognize that to decrypt the encrypted data, one would need only to shift the bits of the encrypted data in a direction opposite the direction used to encrypt the data.

The examiner has interpreted "a number of a terminal" to include an encryption key uniquely associated with each terminal. The use of encryption key is well known by one of ordinary skill at the time of the applicant's invention and disclosed by Nelson, Jr. (col 5, lines 15-20). One of ordinary skill in the art would recognize that it would be more secure if the number of shifts done on each bit of data were determined in some manner by a terminal key or number. As the examiner interprets the claim, one possible purpose of enciphering data is so that if a computer accidentally receives data from a terminal when it was not supposed to, the computer would not be able to decode the data since it would not apply the correct number of bit shifts since the computer expected the data to come from one terminal and instead it came from another. In this manner, terminal data is secured as only when a terminal sends data to the correct computer and the computer uses the correct encryption key or number to decrypt the data from the terminal it expected the data to come from would the computer be able to correctly interpret the data.

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Beasley's invention according to the limitations recited in claim 21. One of ordinary skill would have been motivated to do so for the reasons given above.

**Claim 22:**

Beasley, Crandall, Ostermann, and Nelson do not disclose wherein the at least one shared computer is connected to a second network independent of said network. However, computer systems and networks wherein at least one computer (shared or private) is connected to a further/second network independent of said network have existed before the time applicant's invention was made. One of ordinary skill in the art would have been motivated to connect a shared computer to a further/second independent network as it would allow more access of information for the users of the combination system of Beasley, Crandall, Ostermann, and Nelson. Note the above statement was made in the prior office action and as applicant did not disagree, the examiner assumes applicant agrees with the examiner's statement.

**Claim 23:**

Beasley, Crandall, Ostermann, and Nelson do not disclose wherein the network is the Internet. However, the examiner would like to take official notice that a network being the Internet, which is connected to a computer of any sort has been known to exist before the time of the applicant's invention. One of ordinary skill in the art would be motivated to connect a shared computer to a further independent network as this would allow more access of information for the users of the combination system of Beasley, Crandall, Ostermann, and Nelson. Note the above statement was made in the prior office action and as applicant did not disagree, the examiner assumes applicant agrees with the examiner's statement.

**Claim 24:**

Art Unit: 2135

Beasley, Crandall, Ostermann, and Nelson do not disclose wherein the second network is an intranet. However, the examiner would like to take official notice that a further/second network being an intranet has existed before the time of the applicant's invention. One of ordinary skill in the art would be motivated to connect a shared computer to a further/second independent network as this would allow more access of information for the users of the combination system of Beasley, Crandall, Ostermann, and Nelson. Note the above statement was made in the prior office action and as applicant did not disagree, the examiner assumes applicant agrees with the examiner's statement.

Claims 4, 10, and 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beasley et al (US 5,721,842) in view of Crandall (US 5,159,632) and further in view of Wilder et al (US 6,557,170).

**Claims 4 and 10:**

Beasley further discloses:

1. A switching unit that cancels a connection of the terminal when the terminal has been connected to the shared computer and switches the connection to a private computer corresponding to the terminal, that cancels a connection of the terminal when the terminal has been connected to a private computer corresponding to the terminal and switches the connection to the shared computer (Fig 1, item 60).

Beasley and Crandall do not explicitly disclose the following limitation, which is disclosed by Wilder:

1. A detecting unit that detects whether or not a key code of a predetermined key transmitted from any terminal has been received by a predetermined number during a predetermined period of time (col 2, lines 19-49; col 5, lines 54-64; and col 6, lines 28-35).

Beasley, Crandall, and Wilder do not explicitly disclose the switching unit disregarding the connection switching request when a terminal other than the corresponding terminal has already been connected to the shared computer, at a time when the detecting unit has performed detecting. However, as stated in the last office action, it is well known to disregard a request to connect to a device when the device is busy already. As applicant did not disagree, the examiner assumes the applicant agreed with the examiner's statement. Thus the above limitation is obvious to the combination invention of Beasley, Crandall, and Wilder as it would be unfair to disconnect the first terminal in the middle of whatever it was doing. One of ordinary skill would be motivated to incorporate Wilder's teachings because Wilder's teachings would allow for software switching via the use of "hot keys" (col 5, lines 54-64).

Claim 4 discloses a switching unit which utilizes the methods and steps disclosed by claim 10.

**Claim 25:**

Beasley discloses a computer system comprising at least one private computer; a terminal corresponding to the at least one private computer; at least one shared computer connected to a network; and a switching device disposed between the at least one private computer and the terminal, for relaying data between the terminal and the at least one shared computer (Fig 1), the switching device comprising:

1. A connecting unit that connects each terminal to a corresponding private computer in a default status and a switches destination of the terminal to a private computer corresponding to said terminal or the at least one shared computer when a connection switching request transmitted from said terminal has been received (col 2, lines 56-64).
2. A switching unit that cancels a connection of the terminal when the terminal has been connected to the shared computer and switches the connection to a private computer corresponding to the terminal, that cancels a connection of the terminal when the terminal has been connected to a private computer corresponding to the terminal and switches the connection to the shared computer (Fig 1, item 60).
3. A security unit that executes for each terminal identification processing on the data that has been received from any one terminal and output to the at least one private computer or the at least one shared computer (col 1, lines 45-61 and col 3, lines 4-16).

Beasley does not disclose, but Wilder discloses, the connecting unit comprising:

1. A detecting unit that detects whether or not a key code of a predetermined key transmitted from any terminal has been received by a predetermined number during a predetermined period of time (col 2, lines 19-49; col 5, lines 54-64; and col 6, lines 28-35).

Beasley and Wilder do not explicitly disclose the switching unit disregarding the connection switching request when a terminal other than the corresponding terminal has already been connected to the shared computer, at a time when the detecting unit has performed detecting. However, as stated in the last office action, it is well known to disregard a request to connect to a device when the device is busy already. As applicant did not disagree, the examiner assumes the applicant agreed with the examiner's statement. Thus the above limitation is obvious to the combination invention of Beasley and Wilder as it would be unfair to disconnect the first terminal in the middle of whatever it was doing. One of ordinary skill would be motivated to incorporate Wilder's teachings because Wilder's teachings would allow for software switching via the use of "hot keys" (col 5, lines 54-64).

Beasley and Wilder also do not disclose said identification processing including utilizing an identifier corresponding to a connector through which a terminal is connected to encipher a received key code. However, this limitation reads on the use of public key cryptography, which was well known at the time the applicant's invention was made. Public key cryptography is further disclosed by Crandall (col 1, lines 32-51). In public key cryptography, the key itself is an identifier and corresponds to or verifies the

Art Unit: 2135

identity of the sender or connector from which a message is sent. The reason for this is that the public key is an inverse of the private key, so a message enciphered with one can only be deciphered with the other. If the deciphering is successful, it verifies the identity or source of the message (i.e. enciphered key code). One of ordinary skill would have been motivated to incorporate Crandall's teachings as Crandall discloses that the use of public key encryption would eliminate the difficulties of exchanging a secure enciphering key (col 1, lines 32-34).

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Beasley's invention according to the limitations recited in claim 25. One of ordinary skill would have been motivated to do so for the reasons given above.

**Claims 26-28:**

Claims 26-28 recite limitations substantially similar to the ones recited in claims 22-24 respectively. As such, they are rejected using the same reasoning as for claims 22-24.

Claims 5-6, 11-12, and 29-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beasley et al (US 5,721,842) in view of Crandall (US 5,159,632) and further in view of Onsen (US 6,473,811).

**Claims 5 and 11:**

Beasley and Crandall do not disclose a posting unit that posts a connection status of the shared computer to each terminal. However, Onsen discloses this

limitation (col 1, lines 29-39). One of ordinary skill in the art at the time of the applicant's invention would be motivated to incorporate a posting unit which displays connection status into a switching device as that would allow users to see which computers are already busy/connected to another terminal and thereby know to not waste time trying to connect to the busy computers.

**Claims 6 and 12:**

Beasley and Crandall do not disclose the posting unit posts to each terminal that the shared computer is currently being used, when the shared computer is currently being used. However, this limitation is obvious to the combination invention of Beasley, Crandall, and Onsen as Onsen discloses a posting unit which displays connection status of devices (col 1, lines 29-39). One of ordinary skill would be motivated to post to the status of the shared computer to each terminal for the same reason given in claims 5 and 12.

**Claim 29:**

Beasley discloses a computer system comprising at least one private computer; a terminal corresponding to the at least one private computer; at least one shared computer connected to a network; and a switching device disposed between the at least one private computer and the terminal, for relating data between the terminal and the shared computer (Fig 1), comprising:

1. A connecting unit that connects each terminal to a corresponding private computer in a default status and switches a connection destination of the terminal to a private computer corresponding to said terminal or the at least one

shared computer when a connection switching request transmitted from said terminal has been received (col 2, lines 56-64).

2. A security unit that executes for each terminal identification processing on data that has been received from any one terminal and output to the at least one private computer or the at least one shared computer (col 1, lines 45-61 and col 3, lines 4-16).

Beasley does not disclose said identification processing including utilizing an identifier corresponding to a connector through which a terminal is connected to encipher a received key code. However, this limitation reads on the use of public key cryptography, which was well known at the time the applicant's invention was made. Public key cryptography is further disclosed by Crandall (col 1, lines 32-51). In public key cryptography, the key itself is an identifier and corresponds to or verifies the identity of the sender or connector from which a message is sent. The reason for this is that the public key is an inverse of the private key, so a message enciphered with one can only be deciphered with the other. If the deciphering is successful, it verifies the identity or source of the message (i.e. enciphered key code). One of ordinary skill would have been motivated to incorporate Crandall's teachings as Crandall discloses that the use of public key encryption would eliminate the difficulties of exchanging a secure enciphering key (col 1, lines 32-34).

Beasley and Crandall do not explicitly disclose a posting unit that posts a connection status of the at least one shared computer to each terminal. However,

Art Unit: 2135

Onsen discloses a posting unit which displays connection status of devices (col 1, lines 29-39). One of ordinary skill in the art at the time of the applicant's invention would be motivated to incorporate a posting unit which displays connection status into a switching device as that would allow users to see which computers are already busy/connected to another terminal and thereby know to not waste time trying to connect to the busy computers

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Beasley's invention according to the limitations recited in claim 29. One of ordinary skill would have been motivated to do so for the reasons given above.

**Claims 30-32:**

Claims 30-32 recite limitations substantially similar to the ones recited in claims 22-24 respectively. As such, they are rejected using the same reasoning as for claims 22-24.

**Claim 33:**

Beasley discloses a computer system comprising at least one private computer; a terminal corresponding to the at least one private computer; at least one shared computer connected to a network; and a switching device disposed between the at least one private computer and the terminal, for relating data between the terminal and the shared computer (Fig 1), comprising:

1. A connecting unit that connects each terminal to a corresponding private computer in a default status and switches a connection destination of the

terminal to a private computer corresponding to said terminal or the at least one shared computer when a connection switching request transmitted from said terminal has been received (col 2, lines 56-64).

2. A security unit that executes for each terminal identification processing on data that has been received from any one terminal and output to the at least one private computer or the at least one shared computer (col 1, lines 45-61 and col 3, lines 4-16).

Beasley does not disclose said identification processing including utilizing an identifier corresponding to a connector through which a terminal is connected to encipher a received key code. However, this limitation reads on the use of public key cryptography, which was well known at the time the applicant's invention was made. Public key cryptography is further disclosed by Crandall (col 1, lines 32-51). In public key cryptography, the key itself is an identifier and corresponds to or verifies the identity of the sender or connector from which a message is sent. The reason for this is that the public key is an inverse of the private key, so a message enciphered with one can only be deciphered with the other. If the deciphering is successful, it verifies the identity or source of the message (i.e. enciphered key code). One of ordinary skill would have been motivated to incorporate Crandall's teachings as Crandall discloses that the use of public key encryption would eliminate the difficulties of exchanging a secure enciphering key (col 1, lines 32-34).

Art Unit: 2135

Beasley and Crandall do not explicitly disclose a posting unit that posts a connection status of the shared computer to each terminal, the posting unit for posting to each terminal that the at least one shared computer is currently being used, when the at least one shared computer is currently being connected to any one terminal.

However, Onsen discloses a posting unit which displays connection status of devices (col 1, lines 29-39), therefore the above limitation is rendered obvious because of Onsen's teachings. One of ordinary skill would be motivated to post the connection status of the shared computer to each terminal as that would allow users to see which computers are already busy/connected to another terminal and thereby know to not waste time trying to connect to the busy computers.

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Beasley's invention according to the limitations recited in claim 33. One of ordinary skill would have been motivated to do so for the reasons given above.

**Claims 34-36:**

Claims 34-36 recite limitations substantially similar to the ones recited in claims 22-24 respectively. As such, they are rejected using the same reasoning as for claims 22-24.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

Art Unit: 2135

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

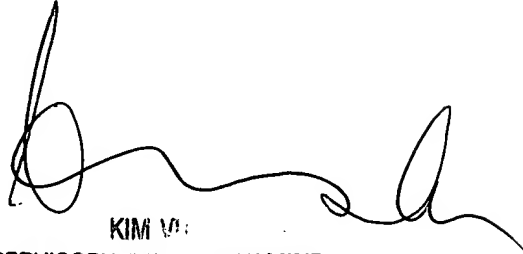
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP



KIM W. [unclear]  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100